UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/654,347	08/30/2000	Douglas B. Moran	RECOP017	5971

21912 7590 03/29/2004

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
BAUM, RONALD	
ART UNIT	**PAPER NUMBER**
2135	7

DATE MAILED: 03/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/654,347	Applicant(s) MORAN, DOUGLAS B.
	Examiner Ronald Baum	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-17 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-17 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 are pending for examination.

2. Claims 1-17 are rejected.

Specification

The disclosure is objected to because of the following informalities: The attempt to incorporate subject matter into this application by reference to US patent applications only by a title (i.e., page 1, lines 10-13, "SYSTEM AND METHOD FOR DETECTING COMPUTER INTRUSIONS", is improper because reference to said documents is incomplete without more specific identification (i.e., actual US patent applications numbers).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Porras et al, U.S. Patent 6,704,874 B1.

5. As per claim 1; "A system for detecting intrusions on a host [col. 1,lines 20-31, col. 2,lines 19-38, col. 3,lines 46-62, col. 12,lines 8-59], comprising: a sensor for collecting

information including events and timestamps from a logfile [col. 1,lines 34-62, col. 52-65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 10,lines 39-45, col. 13,lines 15-23]; and an analysis engine configured to identify backward and forward time steps in the logfile [col. 3,lines 30-40, col. 6,lines 13-col. 7,line 8, col. 12,lines 45-58], correlate the time steps with events, and assign a suspicion value to an event [col. 1,lines 34-col. 2,line 65, col. 6,line 58-col. 7,line 8, col. 8,lines 37-col. 9,line 6]."

6. Claim 2 ***additionally recites*** the limitations that; "The system as recited in claim 1, wherein the analysis engine is configured to identify a time step as forward if a timestamp of an entry in the logfile is later than an preceding entry in the logfile, and identify a time step as backward if a timestamp of an entry in the logfile is earlier than an preceding entry in the logfile.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 8,lines 37-col. 9,line 6, col. 10,lines 39-45, col. 13,lines 15-23) suggest such limitations.

7. Claim 3 ***additionally recites*** the limitations that; "The system as recited in claim 1, wherein the analysis engine is further configured to use expected activity level in the directory to determine the suspicion value.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 8,lines 37-col. 9,line 6, col. 10,lines 39-45, col. 12,lines 8-col. 13,line 23) suggest such limitations.

8. Claim 4 ***additionally recites*** the limitations that; "The system as recited in claim 1, further comprising a second sensor for collecting information including events and timestamps from a second logfile.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 5,lines 63-col. 6,line 13, col. 7,lines 55-66) suggest such limitations.

9. Claim 5 ***additionally recites*** the limitations that; "The system as recited in claim 4, wherein the analysis engine is configured to correlate a time step in the logfile with an event in the second logfile.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 5,lines 63-col. 6,line 13, col. 6,line 58-col. 7,line 8, col. 8,lines 37-col. 9,line 6) suggest such limitations.

10. Claim 6 ***additionally recites*** the limitations that; "The system as recited in claim 1, wherein the analysis engine is further configured to filter out expected time steps from further analysis.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 6,line 58-col. 7,line 8, col. 8,lines 37-col. 9,line 6) suggest such limitations.

11. Claim 7 ***additionally recites*** the limitations that; "The system as recited in claim 6, wherein the analysis engine is configured to filter out expected backward time steps by correlating them to Network Time Protocol adjustments.". The teachings of Porras et al (col. 3,lines 30-40, col. 6,lines 38-57) suggest such limitations.

12. Claim 8 ***additionally recites*** the limitations that; "The system as recited in claim 6, wherein the analysis engine is further configured to compute an expected time drift resulting from a Network Time Protocol adjustment, and compare a forward time step in the logfile with the expected time drift.". The teachings of Porras et al (col. 3,lines 30-40, col. 6,lines 38-57) suggest such limitations.

13. Claim 9 ***additionally recites*** the limitations that; "The system as recited in claim 8, wherein the analysis engine is further configured to compute a standard deviation of the expected time drift.". The teachings of Porras et al (col. 3,lines 30-40, col. 6,lines 38-57, col. 8,lines 37-67) suggest such limitations.

14. Claim 10 ***additionally recites*** the limitations that; "The system as recited in claim 9, wherein the analysis engine is further configured to label time steps with weighted distributions.". The teachings of Porras et al (col. 3,lines 30-40, col. 6,lines 38-57, col. 8,lines 37-67) suggest such limitations.

15. Claim 11 ***additionally recites*** the limitations that; "The system as recited in claim 1, further comprising a user interface, and wherein the analysis engine is configured, upon correlating a time step to a record of an event in a logfile, to present the record to a user for labeling as to suspicion value.". The teachings of Porras et al (col. 7,lines 19-32, col. 9,lines 13-20) suggest such limitations.

16. Claim 12 ***additionally recites*** the limitations that; "The system as recited in claim 11, wherein the analysis engine is further configured to propagate the suspicion value to related events. The teachings of Porras et al (col. 6,lines 27-32, col. 7,lines 19-32,56-67, col. 9,lines 13-20, col. 10,lines 65-67) suggest such limitations.

17. As per claim 13; "A system for detecting intrusions on a host [col. 1,lines 20-31, col. 2,lines 19-38, col. 3,lines 46-62, col. 12,lines 8-59], comprising: a filesystem scanner configured to examine timestamps of files and directories in a filesystem [col. 1,lines 34-62, col. 52-65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 10,lines 39-45, col. 13,lines 15-23]; and an analysis engine configured to compare timestamps of a directory and of files in the directory [col. 3,lines 30-40, col. 6,lines 13-col. 7,line 8, col. 12,lines 45-58], and assign a suspicion value to the directory or file if the timestamps are inconsistent [col. 1,lines 34-col. 2,line 65, col. 6,line 58-col. 7,line 8, col. 8,lines 37-col. 9,line 6. Further, the phrase "...timestamps are *inconsistent*"

(those timestamps encompassed by "inconsistent"), for purposes of the prior art search, it is being presumed that this refers to any timestamps not in forward or backward sequence.].";

18. Claim 14 ***additionally recites*** the limitations that; "The system as recited in claim 13, wherein the analysis engine is configured to treat timestamps as inconsistent if the timestamp of the directory is later than the timestamp of any file in the directory.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 8,lines 37-col. 9,line 6, col. 10,lines 39-45, col. 13,lines 15-23) suggest such limitations.

19. Claim 15 ***additionally recites*** the limitations that; "The system as recited in claim 13, further comprising an archival source, wherein the filesystem scanner is configured to examine timestamps of files and directories from the archival source, and the analysis engine is further configured to compare the timestamps from the *archival* source to the timestamps of the directory and files in the directory.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 8,lines 37-col. 9,line 6, col. 10,lines 39-45, col. 12,lines 8-col. 13,line 14) suggest such limitations.

20. As per claim 16; "A method for detecting intrusions on a host [This claim is an method claim for limitations from the apparatus claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection], comprising the steps of: collecting, information including events and timestamps from a logfile; identifying backward and forward time steps in the logfile; correlating the backward and forward time steps with events; and assigning a suspicion value to an event.";

And further as per claim 17; "A computer program product for detecting intrusions on a host [This claim is an embodied software claim for limitations from the method claim 16 above,

and is rejected for the same reasons provided for the claim 16 rejection], the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of: collecting information including events and timestamps from a logfile; identifying backward and forward time steps in the logfile; correlating the backward and forward time steps with events; and assigning a suspicion value to an event.";

Conclusion

21. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu, can be reached at (703) 305-4393. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner